MEDWIN PUBLISHERS
Committed to Create Value for Researchers

Open Access Journal of Criminology Investigation & Justice
ISSN: 3064-7940

Cyber VAT Fraud in the EU: A Criminological Analysis

Baratto G[1,2], Boriero D[2], Di Nicola A[1,2]* and Perrone G[1,2]

[1]Faculty of Law, University of Trento, Italy

[2]Centre of Security and Crime Sciences, University of Trento and University of Verona, Italy

***Corresponding author:** Andrea Di Nicola, Faculty of Law, University of Trento, Centre of Security and Crime Sciences, University of Trento and University of Verona, Italy, Email: andrea.dinicola@unitn.it

Research Article

Volume 3 Issue 1

Received Date: January 11, 2025

Published Date: January 31, 2025

DOI: 10.23880/oajcij-16000129

Abstract

This article is an anticipation of the criminological analysis of cyber VAT fraud in the European Union carried out in the framework of the project "EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study", co-founded by the Union Anti-Fraud Program (EUAF) of the European Anti-Fraud Office (OLAF). In its empirical criminological perspective, the EU CYBER VAT project investigates behaviors in cyberspace that harm the EU's financial interests through VAT evasion and assesses how digitalization affects the commission of these crimes. More specifically, it investigates how the Internet creates new criminal opportunities for VAT fraud and influences the organization of these crimes, both in terms of criminal activities and the means of communication between network members. To achieve this goal, a script analysis was used to classify the criminal opportunities that the Internet provides to fraudsters; for each criminal activity considered, the script framework was used to determine how the Internet has an impact. Data was collected through case studies, focusing on court cases selected by national experts and relevant stakeholders (e.g. national and supranational authorities and bodies involved in the fight against VAT fraud). The analysis shows, among other things, that the Internet not only facilitates connections between sellers, intermediaries and buyers, but also speeds up transactions and promotes trade by enabling the easy sale of transferable intangible goods. More comprehensive results will be presented in the final report of the project and will contribute to the development of more effective counter measures.

Keywords: Cyber VAT Fraud; Digital Crime; Crime Script; European Union Financial Interests; Criminal Opportunities; Digitalization

Introduction

VAT fraud encompasses a variety of schemes that exploit the Value Added Tax system, broadly categorized according to their objective: reducing tax liability (tax evasion) or misappropriation of VAT through non-payment or false claims for tax credits [1]. These frauds can be very complex, ranging from national cases to international operations with complicated “carousel transactions” that increase the financial damage to the national budget [1].

The fraud becomes even more damaging when several transactions are used to create multiplier effects that cause damage to the public purse through the non-payment and deduction of VAT. The issue here is twofold: firstly, the missing trader invoices VAT to its customer but does not subsequently pay it to the tax authorities, and secondly, the customer can deduct the input VAT paid to the missing trader [2].

Unpaid VAT often serves as the main source of funding for criminal organizations that specialize in this category of

economic and financial crime and use the funds to finance other forms of criminal activity, as will be explained later. In the European Union a common and particularly damaging form is missing trader intra-community fraud (MTIC): a complex and often large-scale form of VAT fraud recognized by Europol [3] as one of the biggest organized crime threats in the EU, affecting all Member States.

An important form of missing trader intra-community fraud (MTIC) is carousel fraud [4], which can be open or closed; the 'closed carousel' represents the "reference form" for this type of fraud, precisely because of this circular shape from which the name 'carousel' originates.

In this scheme, company A (supplier or 'conduit' company) in Member State 1 sells goods or services to company B (missing trader) in Member State 2. In this case, the zero VAT rate applies. Company B sells the goods and services to company C (broker) in Member State 2 and the VAT rate of Member State 2 applies. Company B then disappears without paying the VAT due. Company C then sells the goods or services back to company A in Member State 1. The sale from company C to company A in Member State 1 is an intra-community sale and therefore company C can claim a refund of the VAT paid to company B. Therefore, the budget of Member State 2 suffers a double loss as the missing trader (company B) doesn't pay the VAT due and the intermediary (company C) claims a refund of the VAT paid to the disappeared trader.

This mechanism leads to double financial losses for the state due to unpaid taxes and unjustified VAT refunds [5]. The complexity of these schemes increases with the involvement of buffer companies, which disguise the fraudulent activities and make investigations more difficult. Between the main actors, there may be several buffer companies, some or all of which may be honest [6]. As for the other actors, party (C) involved may also be unaware of the fraudulent scheme, although in any case it is at an advantage by buying from the missing trader (B), as (B) can afford to sell the goods to the domestic trader at a lower price than other competing traders due to the unpaid tax it collects on recovery. While some actors in these chains may not be aware of the fraud, the main actors-suppliers and brokers-are often complicit by using fictitious companies to commit these crimes [7]. The analysis presented here focuses specifically on this type of carousel fraud as a case study because of its importance as a threat to the EU's financial interests.

Despite its significant economic and social consequences, VAT fraud has been largely neglected in criminological research. The field has traditionally focused on white-collar crime and corporate misconduct, leaving a gap in the understanding of VAT fraud as a criminal phenomenon from a criminological perspective rather than an economic and legal one. VAT fraud is becoming an increasingly complex criminal offence that poses a serious threat to the EU's financial interests, as it usually involves large companies and affects various jurisdictions inside and outside the EU market. In its 2023 Annual Report, EPPO assessed the financial impact of VAT fraud on the EU. The results show that VAT fraud accounts for 59% of the total budget lost to the EU due to the crimes investigated by EPPO and amounts to €11.5 billion, 71% more than in 2022.

Digitalization has further exacerbated the problem and created new opportunities for fraudsters. Online transactions enable anonymity, speed and cross-border operations, making detection and enforcement more difficult [8]. Sophisticated technologies such as cryptocurrencies and anonymous payment systems are now frequently used to disguise illicit activities, particularly in the context of e-commerce [9].

In addition, the dematerialization of assets and transactions makes it more difficult to detect criminal activity, as it is difficult for authorities to track the flow of money and goods across the entire chain of exchange. The growth of e-commerce has exacerbated the risks as companies exploit the complexity of cross-border transactions and use methods such as false reporting, failure to register for VAT and invalid VAT numbers to evade taxes [10].

The EU faces an urgent need to address these evolving threats by tackling the technological and operational sophistication of VAT fraud schemes. A deep and thorough understanding of the phenomenon is critical for law enforcement agencies to adapt and respond effectively to these challenges. This analysis aims to contribute to this understanding by examining the digital dimensions of VAT fraud in the European Union to provide insights into the criminal opportunities offered by digitalization.

Aim and Methodology

The aim of this analysis is to examine cyber-VAT fraud (i.e. the digital dimension of VAT fraud) in the European Union through an empirical criminological lens. Starting from the modus operandi of the perpetrators, we wanted to analyze how the Internet affects the different activities and phases that characterize the commission of the crime of VAT fraud in the European Union.

As there is currently no effective and uniform definition of cyber VAT fraud, we have developed the following phenomenological definition of cyber VAT fraud to guide our analysis:

- Cyber VAT fraud involves the use of technology to

facilitate the criminal activity as a whole or to assist in one or more of its stages/phases. The use of technology at one or more stages/phases may include the creation of shell companies using forged documents or identities, the conduct of online transactions and the sale of online goods, including digital goods.

By 'cyber VAT fraud', the authors mean VAT fraud facilitated by new digital technologies/elements, as is the case in many digital organized crime activities [11]. Digital facilitation can take place at various stages (e.g. at the financial transaction stage, where money flows can be facilitated through online transactions); through specific activities (e.g. hacking to steal documents/information, creating fake documents or setting up fake companies through online channels/tools); or through the creation of new digitally generated intangible technologies (e.g. cloud service, software, carbon credits).

To achieve this aim, a qualitative methodology was used, more specifically a script approach applied to criminal cases.

The concept of 'crime scripts' was developed by Cornish [12] to describe the key stages of criminal activity and to make the decision points clearer.

The script approach has had great success in criminological research as it sheds light on the modus operandi of offenders in committing a particular criminal activity by focusing on identifying specific criminal opportunities and explaining how they are exploited [13].

For example, script analysis has mainly been used in the study of predatory crimes such as sexual crimes against women and children, robbery and theft [14-19] and in cases of check and credit card fraud [20,21], employee cybercrime [22], migrant smuggling [23], antiquities trafficking [24], wildlife trafficking [25], terrorism offenses [26], and money laundering [27,28]. Various authors have used this approach to study organized crime [29-34], as recommended in particular by Cornish and Clarke [35].

Some authors have specifically addressed financial crime scripting by adding financial components to the crime scripting method, arguing that it provides valuable insights for analyzing all forms of for-profit crime [36]. Few authors have examined emerging Internet-facilitated fraud using a crime script approach [37], and of the few that have specifically examined VAT fraud facilitated by the Internet, no work was found that uses a crime script approach to analyze VAT fraud and cyber VAT fraud.

For this reason, we have chosen to apply this method to VAT fraud and examine how and where (in which activity/stage) the Internet has facilitated this type of fraud. Indeed, in the context of fraud, this approach provides valuable insights into the operational knowledge of perpetrators that can contribute to the disruption of fraudulent activities, whether they are carried out online or offline [37]. In order to understand the phenomenon and to identify the criminal activities with which this type of fraud is committed, as well as to understand how modi operandi have changed with digitalization, it is essential to examine case studies.

Indeed, this work draws on two data collection strategies [38], namely case studies of VAT fraud offences (particularly court cases) where the use of the Internet played an important role, and two online focus groups with selected national researchers/experts and relevant stakeholders.

In terms of sources and case selection, relevant case studies were initially identified through a preliminary keyword search of the media, online press and online judgment database. Further cases from the different EU countries were collected through institutional contacts, in particular with authorities and officials actively involved in the fight against cyber VAT fraud (e.g. the Italian Guardia di Finanza), as well as through the national researchers involved in the project (one per Member State). A purposive sample was drawn to select the cases to be included in the analysis. Only VAT fraud that concerned Member States of the European Union and in which the Internet played a "significant" role were included. More specifically the criteria for inclusion in the investigation were therefore: 1) a case of VAT fraud affecting the financial interests of the EU; 2) a case of VAT fraud involving at least one cyber element; 3) the source contained details of the cyber elements of the VAT fraud and of the behaviors of the perpetrators.

On the basis of these criteria, 12 cases were selected for analysis, namely 3 Spanish, 2 Italian, 3 Dutch, 1 Lithuanian, 1 Polish, 1 Czech and 1 Belgian. It should be noted that the publicly available case law on VAT fraud is quite limited, especially in relation to cases of fraud enabled and/or facilitated by technology. It was therefore difficult even for the national researchers involved to find suitable examples that matched our research needs.

Searching for cases on the online pages of traditional newspapers and financial newspapers as well as online websites in the hope of finding articles on cases of VAT fraud also revealed descriptions of new cases, but with very limited information, particularly in relation to the digital element. Even when reviewing EPPO press releases and relevant parliamentary questions on VAT fraud, there were few findings on cyber VAT fraud.

Once the cases were identified, cyber VAT fraud was broken down into key stages for investigation. This was

done to determine when and how the Internet is used. To this end, the data was analyzed using a script model based on the work of Hancock and Laycock [31] and Lavorgna [25]. Moving on to the actual script of a carousel fraud, as in Lavorgna's model "The Crime Script for Identifying Internet-Related Criminal Opportunities" [25], the main stages have been identified, including the stages that precede and follow the actual scam. The ten stages are as follows:

- Stage 1: Preparatory activities that precede the commission of the carousel fraud;
- Stage 2: Creation/opening of the "missing trader" to commit the fraud;
- Stage 3: Initial sale: intra-EU VAT-free transaction (A→B);
- Stage 4 (eventual): Multiple resales (B→ Buffer(s) →C);
- Stage 5: Internal sale with VAT (B→C);
- Stage 6: Non-remitting of the collected VAT (by B);
- Stage 7: Disappearance of company B (becoming missing trader) as an exit strategy (activity to evade the authorities);
- Stage 8: Final sale: intra-EU sales without VAT returned to the first seller (C→A);
- Stage 9: Request for refund of VAT paid (by C to B, missing trader);
- Stage 10: Post-fraud activities directly resulting from or following the fraud.

The single actions performed by the fraud actors at each stage were identified in the general "Action" column (see Table 1), and each action was assigned a function using the "sequence of functions in the crime scene" identified by Cornish [12] and described by Hancock and Laycock [31], namely: preparation, entry, precondition, instrumental initiation, instrumental actualization, action, postcondition, and exit.

Indeed, as shown in the table below, from Hancock and Laycock's [31] "integrated organized crime script" model, the labels "function" and "action" were retained and a specific column "Action in which ICTs are used" was added, as in Lavorgna's model [25].

Script Analysis and Interpretation

In the selected cases, several companies (buffers) based in different countries (sometimes even outside the EU) were always involved. However, as already explained, the use of filter companies (buffers) is not necessary for the commission of fraud. In the cases examined, one or more buffers were always interposed to further complicate the tracing of the trade, but this is not necessarily the case in all cyber VAT frauds; for this reason, the function of this action has been referred to as 'eventual' (Table 1). The goods involved – which always belong to the high VAT fraud risk goods, such as technical equipment and digital goods (cloud storage and software) – were only moved at the accounting level (without ever actually being moved), with simulated transactions and false documents (e.g. false invoices). In the selected cases, "paper" companies were repeatedly set up with the aim of committing fraud or purchased on internet platforms: in some of them dormant companies with a broad corporate purpose, that were then converted into paper mills, were bought on websites offering dormant or "silent" companies for sale, even with a "straw man" person as their administrator.

Finally, in some cases, undeclared accounting software was used to track real and fictitious transactions and manage "parallel markets" via separate digital registers. In view of the stages described above, the data have been compiled in the following table (Table 1). This script framework does not include all the actions required to commit VAT carousel fraud (in different types of frauds, such as open frauds), but focuses on those where the Internet was used, as found in the case studies examined. Thus, in the Table, for each stage of VAT fraud (as described in the case studies analyzed), the reader will find the various functions in the activity and the corresponding actions, as well as the type of Internet use in that specific action.

In particular, the script for cyber VAT fraud outlines a series of actions in which the Internet acted as a facilitator. The Table (column Action in which ICTs are used in Table 1) shows how the possibilities of the internet are exploited, both for services (e.g. e-mail providers and instant messaging) and for online "places" (e.g. certain commercial websites) where the services needed to commit fraud can be purchased.

Using this conceptual framework, it was possible to identify five main types of criminal facilitation/opportunity that the Internet provides for the commission of this crime, namely:

- Communicative facilitations/opportunities: communication with suppliers and customers is facilitated by the use of services such as e-mail and Skype;
- Organizational facilitations/opportunities: the use of the Internet facilitates the internal organization of the parties and (if any) the criminal network. The Internet eliminates the need for direct contacts with the actors involved in cross-border trade or with the end users and facilitates contacts between them;
- Information facilitations/opportunities: the Internet makes it possible to access useful information and find out about certain online services that can provide solutions to specific problems. For example, the ability to obtain information about a company (e.g. VAT numbers) or to buy inactive companies to use as missing traders;
- Economic facilitations/opportunities: transferring

funds between bank accounts is done digitally, via online banking systems and using instant transfers, so money can be moved faster;

- Logistical facilitations/opportunities: high-risk goods and digital goods are used, which can be easily moved using only accounting and simulated transactions, without the need for transportation documents or warehouses.

Stage	Function	Action	Action in which ICTs are used
1	Instrumental Initiation	Identify and mapping existing service for purchasing inactive companies or identify how to quickly open a new company	Web research
1	Preparation	Formation / existence of the criminal network with other party	Online contacts (email, Skype)
1	Instrumental Initiation	Recruitment of professionals (e.g. accountants, tax advisors and lawyers and IT specialists)	Online contacts (website, emails)
1	Preparation	Establishing contacts with suppliers and customers	Online contacts (online trading websites, emails, Skype)
2	Instrumental Initiation	Creation of a fictitious company B (missing trader)	Buying inactive companies via certain websites, together with a “straw man” who is used as their administrator to exploit them for fraud
2, 3, 4 and 5	Precondition	Maintenance of contacts with other party	Online contacts (email, Skype)
3	Instrumental actualization	Initial sale VAT-free (A → B)	Buying and selling in e-commerce. Buying and selling can involve digital (intangible) goods
3	Doing	Invoicing initial sale (A → B)	Use of e-invoicing. Creation of false invoices (Internet)
3	Doing	Creation of fake documentation related to initial sale (A → B)	False purchase and sales contracts, false purchase orders and other documents with false information on transactions and business partners created using technology
4	Eventual	Multiple Resales (B → Buffer(s) → C)	Payments by express bank transfer or instant bank transfer with online banking
5	Instrumental actualization	Internal sale VAT-inclusive (B → C)	Buying and selling can take place in electronic commerce. Buying and selling can involve digital (intangible) goods
5	Doing	Invoicing internal sale (B → C)	Use of e-invoicing. Creation of false invoices (Internet)
5	Doing	Creation of fake documentation related to internal sale (B → C)	False purchase and sale agreements, false purchase orders and other documents containing false information about transactions and business partners created with the help of technology
6	Doing	Company B non-remitting the collected VAT	Omitting VAT declarations online
8	Instrumental actualization	Final sale VAT-Free to initial seller (C → A)	Buying and selling can take place in electronic commerce. Buying and selling can involve digital (intangible) goods
9	Instrumental actualization	Company C VAT Refund Claims	Use of e-invoicing for automatic claim
7	Exit	Disappearance of Missing Trader (B)	Fast closing through access to online platforms for company registration and by completing the closing forms directly online
10	Post-condition	Dividing the proceeds of VAT fraud among all actors	Faster and anonymous economic transactions (crypto-currency, block chains) on accounts abroad

Table 1: The crime script for Cyber VAT fraud in the European Union.

Conclusion

The criminological analysis presented here shows the significant impact of digitalization on VAT fraud in the European Union and, in particular, how the Internet facilitates the commission of this crime. Using the script analysis methodology, the study analyzes the different stages of cyber VAT fraud, highlighting the operational methods used by the perpetrators and the criminal opportunities enabled by digital technologies.

The key findings show that the internet plays a crucial role in facilitating communication, organization, financial transactions and logistics for fraudulent schemes. The use of online platforms for the acquisition of shell companies, the creation of false documents using ICT and fast economic transactions through online banking have not only increased the reach and complexity of VAT fraud, but have also brought new challenges for detection and enforcement.

These tools have made it easier for perpetrators to exploit vulnerabilities in VAT systems and conceal their activities from the authorities. As a result, VAT fraud continues to undermine the financial interests of EU Member States, drains significant resources from public budgets and highlights the urgent need for increased prevention and investigation measures.

Increased international cooperation, investment in technological expertise and the introduction of advanced digital tools for real-time tracking are essential to tackle the growing threat of cyber VAT fraud. This work forms the basis for further research into these crimes in the final report of the EU CYBER VAT project, which aims to support more robust and effective measures against this widespread form of financial crime.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgement

Project EU CYBER VAT. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Anti-Fraud Office (OLAF). Neither the European Union nor the granting authority can be held responsible for them.

References

1. Fedeli S, Forte F (2011) EU VAT Frauds. European Journal of Law and Economics 31(2): 143-166.
2. Lamensch M, Ceci E (2018) VAT fraud: Economic impact, challenges and policy issues.
3. Europol (2013) SOCTA EU Serious and Organized Crime Threat Assessment.
4. CEPOL (2022) Carousel Fraud. Serious and organised crime.
5. European Parliament (2021) Missing Trader Intra-Community Fraud. BRIEFING Requested by the CONT Committee, Policy Department for Budgetary Affairs, Directorate-General for Internal Policies.
6. Smith S (2007) VAT fraud and evasion. The IFS Green Budget, pp: 5.
7. Tundo F (2010) Il dolo quale elemento determinante nella repressione alle frodi IVA. Corr. trib., pp: 969.
8. Holt TJ, Lee JR (2023) A crime script model of Dark web Firearms Purchasing. Am J Crim Just 48: 509-529.
9. Borselli F, Fedeli S, Giuriato L (2015) Digital VAT Carousel Fraud: A New Boundary for Criminality.
10. Moiseienko A (2020) Understanding Financial Crime Risks in E-Commerce. RUSI Occasional Paper, pp: 2-10.
11. Di Nicola A (2022) Towards digital organized crime and digital sociology of organized crime. Trends Organ Crim.
12. Cornish DB (1994) The procedural analysis of offending and its relevance for situational prevention. In: Clarke RV (Eds.), Crime Prevention Studies, New York: Criminal Justice Press, pp: 3.
13. Lavorgna A (2014) Script analysis of complex criminal activities: Investigating the use of the internet as a facilitator for offline transit crimes. In Sage Research Methods Cases Part 1. SAGE Publications, Ltd.
14. Tremblay P, Talon B, Hurley D (2001) Body switching and related adaptations in the resale of stolen vehicles. British Journal of Criminology 41(4): 561-579.
15. Petrosino A, Brensilber D (2003) The motives, methods and decision making of convenience store robbers: Interviews with 28 incarcerated offenders in Massachusetts. In: Smith MJ, Cornish DB (Eds.), Theory for practice in situational crime prevention. Crime Prevention Studies, No. 16. Monsey (NJ): Criminal Justice Press.
16. Smith MJ (2005) Robbery of taxi drivers. Problem-specific Guides Series, pp: 34.
17. Chiu YN, Leclerc B (2017) An Examination of Sexual

Offenses Against Women by Acquaintances: The Utility of a Script Framework for Prevention Purposes. In: Leclerc B, Savona E (Eds.), Crime Prevention in the 21st Century. Springer, Cham.

18. Chopin J, Beauregard E (2020) Scripting Extrafamilial Child Sexual Abuse: A Latent Class Analysis of the Entire Crime-Commission Process. Child Abuse & Neglect 106: 104521.

19. Van der Bruggen M, Blokland A (2021) A Crime Script Analysis of Child Sexual Exploitation Material Fora on the Darkweb. Sexual Abuse 33(8): 950-974.

20. Mativat F, Tremblay P (1997) Counterfeiting credit cards: Displacement effects, suitable offenders and crime wave patterns. The British Journal of Criminology 37(2): 165-183.

21. Lacoste J, Tremblay P (2003) Crime and innovation: A script analysis of patterns in check forgery. In: Smith MJ, Cornish DB (Eds.), Theory for practice in situational crime prevention studies, Monsey (NY): Criminal Justice Press, Vol: 16.

22. Willison R (2006) Understanding the offender/ environment dynamic for computer crimes. Information Technology People 19(2): 170-186.

23. Sarrica F (2005) The smuggling of migrants. A flourishing activity of transnational organized crime. Crossroads 5(3): 7-23.

24. Weirich CA (2019) Situational crime prevention of antiquities trafficking: a crime script analysis. PhD thesis.

25. Lavorgna A (2014) Wildlife trafficking in the Internet age. Crime Sci 3: 5.

26. Clarke RV, Newman GR (2006) Outsmarting the Terrorists. Westport (CT): Praeger Security International.

27. Morselli C, Roy J (2008) Brokerage qualifications in ringing operations. Criminology 46(1): 71-98.

28. Gilmour N (2014) Understanding Money Laundering – A Crime Script Approach. SGOC Studying Group on Organised Crime.

29. Morgenthaler E, Leclerc B (2023) Crime script analysis of drug importation into Australia facilitated by the dark net. Global Crime 24(3): 169-194.

30. Chainey SP, Alonso Berbotto A (2022) A structured methodological process for populating a crime script of organized crime activity using OSINT. Trends in Organized Crime 25: 272-300.

31. Hancock G, Laycock G (2010) Organised crime and crime scripts: prospects for disruption. In: Bullock K, et al. (Eds.), Situational Prevention of Organised Crimes. Devon (UK): Willan Publishing.

32. Chiu YN, Leclerc B, Townsley M (2011) Crime script analysis of drug manufacturing in clandestine laboratories. British Journal of Criminology 51(2): 355-374.

33. Tompson L, Chainey S (2011) Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy. European Journal of Criminal Policy and Research 17(3): 179-201.

34. Savona EU (2010) Infiltration of the public construction industry by Italian organised crime. In: Bullock K, et al. (Eds.), Situational Crime Prevention of Organised Crimes. Abingdon: Willan Publishing.

35. Cornish DB, Clarke RV (2002) Analyzing organized crime. In: Piquero AR, Tibbetts SG (Eds.), Rational choice and criminal behavior: Recent research and future challenges. New York: Routledge.

36. Snaphaan T, van Ruitenburg T (2025) Financial crime scripting: An analytical method to generate, organise and systematise knowledge on the financial aspects of profit-driven crime. European Journal on Criminal Policy and Research pp: 1-21.

37. Leclerc B, Morgenthaler E (2023) Examining emerging fraud facilitated by the internet through crime scripts. Trends & Issues in Crime and Criminal Justice, Canberra: Australian Institute of Criminology, pp: 680.

38. Hagan FE (2011) Research method in criminal justice and criminology. Upper Saddle River (NJ): Prentice Hall.